

第5回 サイバーセキュリティ検証基盤構築に向けた有識者会議

日時・場所 令和2年2月19日(水) 13:00-15:00 独立行政法人情報処理推進機構 (IPA)

出席者

[委員] 熱海委員、高倉委員、斉藤委員、寺原委員、名和委員、政本委員

[事務局] IPA セキュリティセンター 瓜生センター長、小川グループリーダー、増田主任研究員

[オブザーバー] 経済産業省 商務情報政策局 サイバーセキュリティ課 鴨田企画官、西野課長補佐、入江課長補佐、野村係長

議事概要

第5回の会議では、IPA より緑検証(対象製品: yamory)、青検証(対象製品: AX-Network-Visualization(AX-NV))の中間報告と、重要分野マップ、今後のスケジュール等について説明。その後、中間報告の内容などについて自由討議を行った。委員からの意見は以下の通り。

【緑検証の中間報告内容について】

- yamory の独自のトリアージ機能は、JPCERT/CC が 2007 年に開発した「KENGINE」に似ている。知っている人は知っているのですが、何が「独自」かと問われた時に説明できるようにしておいた方が良いでしょう。
- yamoryの脆弱性付加情報の内容を詳しく知りたい。自社で採用している海外製の脆弱性スキャナーとの特徴的な違いを知りたい。
- Tenable等のネットワークスキャナとyamoryを比較すると、yamoryはOSSの依存関係を見るものでDev opps系に使うという違いがある。優先度付けは、システムが公開されている(グローバルIPがある)、PoCが公開されている、CVSSのスコアが高いの3点で行う。
- ディベロッパーの開発チームが必要最低限のアクションを取れるように特化しているもので、多機能だがセキュリティ専門家でないと使いこなせないような難しいツールになっていないのが良い点。

【青検証の中間報告内容について】

- 検証項目に「IoT」とあるが、想定している適用分野は家庭用などの小さいエリアのものなのか、工場などのエリアが広いものまで入るのか。
 - 特に限定していないので、家庭用などの小規模から工場など大規模のIoTも適用範囲。
 - IoTの範疇にLPWPのノード機器も入ってくるので、そこも対象に見ておいた方がよい。
 - クラウドネットワークへの接続点(ノード)が外部から見える利用例がいくつかある。そこも対象になると考えられる。
 - そのようなリスクはローカル5Gやプライベート5Gになると低減されるものなのか？
 - ローカル5Gを使って、ケーブルを無くしたケーブルテレビTVが外国から日本に押し寄せてきている。
- 新しいテクノロジーがどんどん来ると、こういう製品もタイムリーに出していかないと周回遅れになる。
- 適用対象にEDIも検討するべき。専用線が利用できなくなるため、IoTやインターネット化などが見え隠れしているが、セキュリティ対策が不十分なところが多い。
- 通信の大半がHTTPSになり、パターンマッチングでは攻撃を検知できなくなっている。AX-NVのような通信の挙動を見るツール(と脅威インテリジェンス)が必要。

【成果公表について】

- 最終的な今年度成果公表の公開コンテンツについては、メールベースで委員の皆様にご展開し、ご確認いただくことで了承いただいた。

以上